IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A method [[for]] of encrypting an input data string ~~comprising~~ including a plurality of bits of binary data ~~using~~ with a processing device ~~including a processor~~ communicatively coupled to a memory ~~loaded with~~ having an encryption program stored therein, the method comprising:

receiving an input data string for encryption at ~~a processor~~ the processing device;

providing a ~~static~~ control code index ~~that is~~ in the memory, the control code index being defined prior to receiving the input data string for encryption at the ~~processor~~ processing device, the control code index including a plurality of control codes ~~wherein the values of the plurality of control codes are independent of input data string specific characteristics~~;

determining an order in which to query the presence of each of 2^n different configurations of n bits within an input data string;

generating a control code associated with the determined order using the control code index, the values of the generated control code being independent of input data string specific characteristics;

generating a position code by identifying positions of each of the 2^n different configurations of n bits in the input data string in accordance with the determined order; and

combining the control code and the position code to form an encrypted data string.

Claim 2 (Canceled).

Claim 3 (Previously Presented): The method of Claim 1, wherein determining an order comprises selecting a predetermined order.

Claim 4 (Canceled).

Claim 5 (Currently Amended): The method of Claim 1, further comprising:

dividing the input data string into a plurality of blocks of data.

Claim 6 (Previously Presented): The method of Claim 5, wherein the number of bits within each of the plurality of blocks of data is individually determined in response to a random number generator.

Claim 7 (Previously Presented): The method of Claim 5, wherein the number of bits within each of the plurality of blocks of data is individually determined in response to a mathematical formula.

Claim 8 (Currently Amended): The method of Claim 5, further comprising:

generating a plurality of block codes associated with a plurality of blocks of data of the input data string, each block code indicating the number of bits within the associated block of data.

Claim 9 (Currently Amended): The method of Claim 8, further comprising:

combining the each of the plurality of block codes with the control code and the position code for the associated block of data.

Claim 10 (Previously Presented): The method of Claim 1, wherein determining an order comprises determining an order based on the frequencies of the 2^n combinations of the n bits of the input data string.

Claims 11-20 (Canceled).

Claim 21 (Currently Amended): A method for encrypting an input data string, ~~comprising~~ including a plurality of bits of binary data, the method comprising:

~~using a software program code means embodied on a computer readable medium,~~ receiving an input data string for encryption;

~~using a software program code means embodied on a computer readable medium,~~ providing a ~~static~~ control code index ~~that is~~, the control code index being defined prior to receiving the input data string for encryption~~, the control code index including a plurality of control codes wherein the values of the~~, the control code index including a plurality of control codes ~~are independent of input data string specific characteristics~~;

~~using a software program code means embodied on a computer readable medium,~~ determining an order in which to query the presence of each of 2^n different configurations of n bits within an input data string;

~~using a software program code means embodied on a computer readable medium,~~ generating a control code associated with the determined order using the control code index, the values of the generated control code being independent of input data string specific characteristics;

~~using a software program code mans embodied on a computer readable medium,~~ generating a position code by identifying positions of each of the 2^n different configurations of n bits in an input data string in accordance with the determined order; and

~~using a software program code means embodied on a computer readable medium,~~ combining the control code and the position code to form an encrypted data string.

Claim 22 (Currently Amended): The method of Claim 21, further comprising ~~using a software program code means embodied on a computer readable medium,~~

arranging the input data string into a plurality of data blocks.

Claim 23 (Currently Amended): A computer ~~usable~~ readable medium ~~storing a~~ including computer program instructions that cause a computer to implement a method of encrypting an input data string, ~~comprising~~ including a plurality of bits of binary data, the ~~medium~~ method comprising:

~~computer readable code for~~ receiving an input data string for encryption;

~~computer readable code for~~ providing a ~~static~~ control code index that is defined prior to receiving the input data string for encryption, the control code index including a plurality of control codes ~~wherein the values of the plurality of control codes are independent of the input data string specific characteristics~~;

~~computer readable code for~~ determining an order in which to query the presence of each of 2^n different configurations of n bits within an input data string;

~~computer readable code for~~ generating a control code associated with the determined order using the control code index, the values of the generated control code being independent of input string specific characteristics;

~~computer readable code for~~ generating a position code by identifying the positions of each of the 2^n different configurations of n bits in the input data string in accordance with the determined order; and

~~computer readable code for~~ combining the control code and the position code to form an encrypted data string.

Claim 24 (Canceled).

Claim 25 (Currently Amended): The ~~computer usable medium~~ method of Claim 23, wherein ~~the computer readable code for~~ determining an order ~~comprises computer readable code for~~ includes selecting a predetermined order.

Claim 26 (Currently Amended): The ~~computer usable medium~~ method of Claim 23, further comprising ~~computer readable control for~~:

dividing the input data string into a plurality of blocks of data.

Claim 27 (Currently Amended): The ~~computer usable medium~~ method of Claim 26, wherein ~~the computer readable code for~~ dividing the input data string into a plurality of blocks of data ~~comprises computer readable code for~~ includes determining the individual number of bits within each of the plurality of blocks of data in response to a random number generator.

Claim 28 (Currently Amended): The ~~computer readable usable medium~~ method of Claim 26, wherein ~~the computer readable code for~~ dividing the input data string into a

plurality of blocks of data, ~~comprises computer readable code for~~ includes determining the individual number of bits within each of the plurality of blocks of data in response to a mathematical formula.

Claim 29 (Currently Amended): The ~~computer usable medium~~ method of Claim 26, wherein ~~the computer readable code for~~ determining an order further comprises:

~~computer readable code for~~ determining a first order associated with a first block of data and determining a second order associated with a second block of data wherein the first order is different than the second order.

Claim 30 (Currently Amended): The ~~computer usable medium~~ method of Claim 26, further comprising:

~~computer readable code for~~ generating a plurality of block codes associated with a plurality of blocks of data, each block code indicating the number of bits within the associated block of data.

Claim 31 (Currently Amended): The ~~computer usable medium~~ method of Claim 30, further comprising:

~~computer readable code for~~ combining the each of the plurality of block codes with the control code and the position code for the associated block of data.

Claim 32 (Currently Amended): The ~~computer usable medium~~ method of Claim 23, wherein ~~the computer readable code for~~ determining an order ~~comprises computer readable~~

~~code for~~ includes determining an order based on the frequencies of the 2^n combinations of the n bits of the input data string.

Claim 33 (Currently Amended): The ~~computer usable medium~~ method of Claim 23, wherein ~~the computer readable code for~~ determining an order ~~further comprises computer readable code for~~ includes determining an order in which to query the presence of each of 2^n different configurations of n bits based on an analysis of the input data string.

Claim 34 (Currently Amended): The ~~computer usable medium~~ method of Claim 23, wherein ~~the computer readable code for~~ generating the control code ~~comprises computer readable code for~~ includes generating a control code via a random number generator using the control code index.

Claim 35 (Currently Amended): The ~~computer usable medium~~ method of Claim 23, wherein ~~the computer readable code for~~ determining an order ~~comprises computer readable code for~~ includes generating an order using a mathematical formula.

Claim 36 (Currently Amended): The ~~computer usable medium~~ method of Claim 23, further comprising:

~~computer readable code for~~ determining whether the input data string can be compressed simultaneously as it is encrypted.

Claim 37 (Currently Amended): The ~~computer usable medium~~ method of Claim 23, further comprising:

~~computer readable code for~~ dividing the input data string into n bit sequences;

~~computer readable code for~~ comparing each of the 2^n different configurations of n bits with each of the n bit sequences;

~~computer readable code for~~ determining the frequency of each of the 2^n different configurations appearing in the input data string;

~~computer readable code for~~ determining whether a specific relationship exists between values of the frequencies of each of the individual 2^n different configurations appearing in the input data string wherein the existence of the specific relationship is indicative of the presence of a characteristic within the input data string and wherein the presence of the characteristic indicates that the input data string can be compressed simultaneously as it is encrypted;

~~computer readable code for~~ selecting a first position code routine associated with the determined order when the specific relationship exists, the first position code being operable to simultaneously encrypt and compress the input data string; and

~~computer readable code for~~ selecting a second position code routine associated with the determined order when the specific relationship does not exist, the second position code being operable to encrypt the input data string without any compression.

Claim 38 (Currently Amended): The ~~computer usable medium~~ method of Claim 23, wherein ~~the computer readable code for~~ determining the order in which to query the presence of each of 2^n different configurations of n bits within an input data string ~~comprises computer readable code for~~ includes determining the order in which to query the presence of each of 2^2 different configurations of 2 bits within an input data string.

Claim 39 (Currently Amended): The ~~computer usable medium~~ method of Claim 38, further comprising:

~~computer readable code for~~ dividing the input data string into n bit sequences;

~~computer readable code for~~ comparing each of the 2^n different configurations of n bits with each of the n bit sequences of the input data string;

~~computer readable code for~~ determining a first number representative of the number of times the most frequency occurring 2^n configuration appears in the input string.

~~computer readable code for~~ determining a second number representative of the number of times the second most frequency occurring 2^n configuration appears in the input string;

~~computer readable code for~~ determining a third number representative of the number of times the third most frequency occurring 2^n configuration appears in the input string;

~~computer readable code for~~ determining a fourth number representative of the number of times the fourth most frequency occurring 2^n configuration appears in the input string;

~~computer readable code for~~ selecting a first position code routine associated with the determined order when the first number is greater than the sum of the third number and the fourth number thereby indicating the presence of a characteristic that indicates that the input data string can be simultaneously encrypted and compressed, the first position code routine being operable to simultaneously encrypt and compress the input data string; and

~~computer readable code for~~ selecting a second position code routine associated with the determined order when the first number is not greater than the sum of the third number and the fourth number thereby indicating the absence of the characteristic that indicates that the input data string can be simultaneously encrypted and compressed, the second position code routine being operable to encrypt the input data string without any compression.

Claim 40 (Currently Amended): The ~~computer usable medium~~ method of Claim 39, wherein ~~the computer readable code for~~ generating a control code associated with the determined order, further comprises:

~~computer readable code for~~ generating a first control code associated with the determined order when the first position code routine is selected; and

~~computer readable code for~~ generating a second control code associated with the determined order when the second position code routine is selected wherein the first control code is different than the second control code.

Claim 41 (Currently Amended): The ~~computer usable medium~~ method of Claim 23, further comprising ~~computer readable code for~~ encrypting the encrypted data string.

Claim 42 (Currently Amended): The ~~computer usable medium~~ method of Claim 41, wherein ~~the computer readable code for~~ encrypting the encrypted data string comprises:

~~computer readable code for~~ providing an encryption key having a first selected number of bits; and

~~computer readable code for~~ performing an XOR function between the encryption key and the encrypted data string.

Claim 43 (Currently Amended): The ~~computer usable medium~~ method of Claim 41, wherein ~~the computer readable code for~~ encrypting the encrypted data string comprises:

~~computer readable code for~~ determining an order in which to query the presence of each of 2^n different configuration of n bits with the encrypted data string;

~~computer readable code for~~ generating a control code associated with the determined order of the encrypted data string;

~~computer readable code for~~ generating a position code by identifying the positions of each of the 2^n different configurations o n bits in the encrypted data string in accordance with the determined order; and

~~computer readable code for~~ combining the newly generated position code and the newly generated control code to create and encrypted version of the encrypted data string.

Claim 44 (Currently Amended): The ~~computer usable medium~~ method of Claim 25, wherein ~~the computer readable code for~~ selecting a predetermined order ~~comprises~~ includes computer readable code for selecting a default order.

Claim 45 (Currently Amended): The ~~computer usable medium~~ method of Claim 32, wherein ~~the computer readable code for~~ determining an order based on the frequencies of the 2^n combinations of the n bits of the input data string ~~comprises computer readable code for~~ includes determining an order based on the relative frequencies of the 2^n combinations of the n bits of the input data string.

Claim 46 (Currently Amended): The ~~computer usable medium~~ method of Claim 32, wherein ~~the computer readable code for~~ determining an order based on the frequencies of the 2^n combinations of the n bits of the input data string ~~comprises computer readable code for~~ includes determining a pre-determined order based on the frequencies of the 2^n combinations of the n bits of the input data string.

Claim 47 (Currently Amended): The method of Claim 1, wherein determining an order ~~further comprises~~ includes determining an order in which 2^n different configurations of n bits are to be identified in a position code based on an analysis of the input data string.

Claim 48 (Currently Amended): The method of Claim 1, wherein generating the control code ~~comprises~~ includes generating a control code via a random number generator using the control code index.

Claim 49 (Currently Amended): The method of Claim 1, wherein determining an order ~~comprises~~ includes generating an order using a mathematical formula.

Claim 50 (Currently Amended): The method of Claim 5, wherein determining an order ~~further comprises~~ includes determining a first order associated with a first block of data and determining a second order associated with a second block of data wherein the first order is different than the second order.

Claim 51 (Currently Amended): The method of Claim 1, further comprising:

determining whether the input data string can be compressed simultaneously as it is encrypted.

Claim 52 (Currently Amended): The method of Claim 1, further comprising:

dividing the input string into n bit sequences;

comparing each of the 2^n different configurations of n bits with each of the n bit sequences;

determining the frequency of each of the 2^n different configurations appearing in the input data string;

determining whether a specific relationship exists between values of the frequencies of each of the individual 2^n different configurations appearing in the input [[date]] data string wherein the existence of the specific relationship is indicative of the presence of a characteristic within the input data string and wherein the presence of the characteristic indicates that the input data string can be compressed simultaneously as it is encrypted;

selecting a first position code routine associated with the determined order when the specific relationship exists, the first position code being operable to simultaneously encrypt and compress the input data strong; and

selecting a second position code routine associated with the determined order when the specific relationship does not exist, the second position code being operable to encrypt the input data string without any compression.

Claim 53 (Currently Amended): The method of Claim 1, wherein determining the order in which to query the presence of each of 2^n different configurations of n bits within an input data string ~~comprises~~ includes determining the order in which to query the presence of each of 2^2 different configurations of 2 bits within an input data string.

Claim 54 (Previously Presented); The method of Claim 53, further comprising:

dividing the input data string into n bit sequences;

comparing each of the 2^n different configuration of n bits with each of the n bit sequences of the input data string;

determining a first number representative of the number of times the most frequency occurring 2^n configuration appears in the input string;

determining a second number representative of the number of times the second most frequency occurring 2^n configuration appears in the input string;

determining a third number representative of the number of times the third most frequently occurring 2^n configuration appears in the input string;

determining a fourth number representative of the number of times the fourth most frequency occurring 2^n configuration appears in the input string;

selecting a first position code routine associated with the determined order when the first number is greater than the sum of the third number and the fourth number thereby indicating the presence of a characteristic that indicates that the input data string can be simultaneously encrypted and compressed, the first position code routine being operable to simultaneously encrypt and compress the input data string; and

selecting a second position code routine associated with the determined order when the first number is not greater than the sum of the third number and the fourth number thereby indicating the absence of a characteristic that indicates that the input data string can be simultaneously encrypted and compressed, the second position code routine being operable to encrypt the input data string without any compression.

Claim 55 (Previously Presented): The method of Claim 54, wherein generating a control code associated with the determined order, further comprises:

generating a first control code associated with the determined order when the first position code routine is selected; and

generating a second control code associated with the determined order when the second position code routine is selected wherein the first control code is different than the second control code.

Claim 56 (Currently Amended): The method of Claim 1, further comprising:

encrypting the encrypted data string.

Claim 57 (Currently Amended): The method of Claim 56, wherein encrypting the encrypted data string, further ~~comprises~~ comprising:

providing an encryption key having a first selected number of bits; and

performing an XOR function between the encryption key and the encrypted data string.

Claim 58 (Currently Amended): The method of Claim 56, wherein encrypting the encrypted data, further ~~comprises~~ comprising:

determining an order in which to query the presence of each of 2^n different configurations of n bits within the encrypted data string;

generating a control code associated with the determined order for the encrypted data string;

generating a position code by identifying positions of each of the 2^n different configurations of n bits in the encrypted data string in accordance with the determined order; and

combining the newly generated position code and the newly generated control code to create an encrypted version of the encrypted data string.

Claim 59 (Currently Amended): The method of Claim 3, wherein selecting a predetermined order ~~comprises~~ includes selecting a default order.

Claim 60 (Currently Amended): The method of Claim 10, wherein determining an order based on the frequencies of the 2^n combinations of the n bits of the input data string ~~comprises~~ includes determining an order based on the relative frequencies of the 2^n combinations of the n bits of the input data string.

Claim 61 (Currently Amended): The method of Claim 10, wherein determining an order based on the frequencies of the 2^n combinations of the n bits of the input data string ~~comprises~~ includes determining a pre-determined order based on the frequencies of the 2^n combinations of the n bits of the input data string.

Claim 62 (New): An electronic device for encrypting an input data string, including a plurality of bits of binary data, comprising:

a processor configured to receive an input data string for encryption;

a memory configured to include a control code index, the control code index being defined prior to reception of the input data string for encryption by the processor, the control code index including a plurality of control codes, the control codes having corresponding values,

wherein the processor is operably linked to the memory for determining upon reception of the input data string, an order in which to query the presence of each of two 2^n different configurations of n bits within an input data string, and generates a control code

associated with the determined order by access of the control code index in which the corresponding values of the generated control code is independent of the input data string characteristics, the processor generating a position code, through the identification of positions of each of the two 2^n different configurations of n bits in the input data string in accordance with the determined order to combine the control code and the position code to form an encrypted data string.